CLAIMS

Please amend the pending claims as follows.

1. (Currently Amended) A method operational in a mobile user device for authentication in a public cryptographic system comprising:

creating a first private key and corresponding first public key at the mobile user device;

creating a second private key associated with the first private key and creating a second public key corresponding to the second private key at the mobile user device;

wirelessly transmitting a plurality of shares of the second private key to a plurality of different entities ~~once~~ once, such that ~~it~~ the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created;

wirelessly transmitting the second public key to a verifier device concurrent with the first public key; and

using the first private key for authentication of the mobile user device.

2. (Previously Presented) The method of claim 1, wherein wirelessly transmitting the second public key comprises:

creating at least two shares of the second private key at the mobile user device; and

wirelessly outputting each share once to a different entity.

3. (Currently Amended) The method of claim 1, further comprising:

re-creating the second private key at the mobile user device using the plurality of shares; and

using the second private key for authentication of the mobile user device.

4. (Previously Presented) The method of claim 3, further comprising:

disabling the first private key when the second private key is used for authentication of the mobile user device.

5. (Previously Presented) The method of claim 3, further comprising:

creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

outputting the third public key from the mobile user device.

6. (Previously Presented) The method of claim 5, further comprising:

outputting the third private key once such that it can be re-created; and

re-creating the third private key at the mobile user device and using the third private key for authentication.

7. (Previously Presented) The method of claim 1,

wherein the second public and private keys are created independently from the first public and private keys.

8. (Original) The method of claim 3, further comprising:

creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

outputting the fourth private key once such that it can be re-created; and

outputting the third and fourth public keys.

9. (Previously Presented) The method of claim 8, further comprising:

disabling use of the second private key for authentication; and

using the third private key for authentication;

re-creating the fourth private key; and

using the fourth private for authentication.

10. (Previously Presented) The method of claim 1,

preventing retransmission of the second private key.

11. (Currently Amended) A method for verification in a public cryptographic system comprising:

wirelessly receiving a first public key from a mobile user device;

wirelessly receiving a second public key from the mobile user device concurrent with receipt of the first public key, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created by the mobile user device to replace use of a first private key corresponding to the first public key and disable the first private key when the second private key is re-created;

using the first public key for authentication of the mobile user device; and

using the second public key for authentication of the mobile user device if the first public key fails.

12. (Previously Presented) The method of claim 11, further comprising:

receiving a third public key from the mobile user device, the third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

13. (Previously Presented) The method of claim 11, further comprising:

receiving a third public key and a fourth public key from the mobile user device, if the first public key fails and if the second public key results in a successful authentication, wherein the third and the fourth public keys are associated with the second key.

14. (Currently Amended) A mobile user device configured for authentication in a public cryptographic system comprising:

means for creating a first private key and corresponding first public key at the mobile user device;

means for creating a second private key associated with the first private key and creating a second public key corresponding to the second private key at the mobile user device;

means for wirelessly outputting a plurality of shares of the second private key to a plurality of different entities once such that ~~it~~ the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created;

means for wirelessly outputting the second public key to a verifier device concurrent with outputting the first public key; and

means for using the first private key for authentication.

15. (Previously Presented) The device of claim 14, wherein means for wirelessly outputting the second public key comprises:

means for creating at least two shares of the second private key at the mobile user device; and

means for wirelessly outputting each share once to a different entity, wherein subsequent outputting of the second private key is prevented.

16. (Currently Amended) The device of claim 14, further comprising:

means for re-creating the second private key at the mobile user device using the plurality of shares; and

means for using the second private key for authentication of the mobile user device.

17. (Previously Presented) The device of claim 16, further comprising:

means for creating a third private key associated with the second private key and creating a third public key corresponding to the third private key; and

means for wirelessly outputting the third public key to the verifier device.

18. (Previously Presented) The device of claim 16, further comprising:

means for creating a third private key associated with the second key and creating a third public key corresponding to the third private key;

means for creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key;

means for wirelessly outputting the fourth private key once such that it can be re-created; and

means for wirelessly outputting the third and fourth public keys to the verifier device.

19. (Currently Amended) A verifier apparatus configured for verification in a public cryptographic system comprising:

means for wirelessly receiving a first public key from a mobile user device;

means for wirelessly receiving a second public key from the mobile user device concurrent with receipt of the first public key, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created by the mobile user device to replace use of a first private key corresponding to the first public key and disable the first private key when the second private key is re-created;

means for using the first public key for authentication of the mobile user device; and

means for using the second public key for authentication of the mobile user device if the first public key fails.

20. (Previously Presented) The apparatus of claim 19, further comprising:

means for receiving a third public key associated with the second public key from the mobile user device, if the first public key fails and if the second public key results in a successful authentication of the mobile user device.

21. (Previously Presented) The apparatus of claim 19, further comprising:

means for receiving a third public key and a fourth public key, if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second public key.

22. (Currently Amended) A machine-readable medium comprising instructions for performing a public cryptography, which when executed by a processor causes the processor to:

create a first private key and corresponding first public key at a mobile user device;

create a second private key associated with the first private key and creating a second public key corresponding to the second private key at a mobile user device;

wirelessly output a plurality of shares of the second private key to a plurality of different entities once such that ~~it~~ the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created;

wirelessly output the second public key to a verifier device concurrent with outputting the first public key; and

use the first private key for authentication of the mobile user device.

23. (Previously Presented) The machine-readable medium of claim 22, wherein outputting the second private key further comprises instructions to:

create at least two shares of the second private key; and

output each share once to a different entity.

24. (Previously Presented) The machine-readable medium of claim 22 further comprising instructions to:

recreate the second private key; and

use the second private key for authentication.

25. (Previously Presented) The machine-readable medium of claim 24 further comprising instructions to:

disable the first private key by using the second private key for authentication

26. (Currently Amended) A machine-readable medium comprising instructions for performing a public cryptography at a verifier device, which when executed by a processor causes the processor to:

wirelessly receive a first public key from a mobile user device;

wirelessly receive a second public key from the mobile user device concurrent with receipt of the first public key, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created by the mobile user device to replace use of a first private key corresponding to the first public key and disable the first private key when the second private key is re-created;;

use the first public key for authentication of the mobile user device; and

use the second public key for authentication of the mobile user device if the first public key fails.

27. (Previously Presented) The machine-readable medium of claim 26 further comprising instructions to:

wirelessly receive a third public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

28. (Previously Presented) The machine-readable medium of claim 26 further comprising instructions to:

wirelessly receive a third public key and a fourth public key associated with the second public key, if the first public key fails and if the second public key results in a successful authentication.

29. (Previously Presented) A method operational on a mobile user device for authentication in a public cryptographic system comprising:

creating a private key, a public key corresponding to the private key, and an associated system parameter on the mobile user device;

wirelessly outputting the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device; and

using the private key for authentication of the mobile user device.

30. (Previously Presented) The method of claim 29, further comprising:
creating a new private key using a previous private key and the system parameter; and
using the new private key for authentication of the mobile user device.

31. (Original) The method of claim 29, further comprising:
creating a counter value indicating the generation of public and private keys; and
outputting the counter value when outputting the public key.

32. (Original) The method of claim 31, further comprising:
creating the new private key using a previous private key and the system parameter based on the counter value; and
using the new private key for authentication.

33. (Previously Presented) A method operational on a verifier device for verification in a public cryptographic system comprising:
wirelessly receiving a public key from a mobile user device;
wirelessly receiving a system parameter from the mobile user device concurrent with receipt of the public key, the system parameter associated with the public key;
authenticating the mobile user device using the public key; and
generating a new public key at the verifier device and authenticating the mobile user device using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

34. (Original) The method of claim 33, wherein generating the new public key comprises:
using a number of powers of the previous public key for authentication; and
accepting one that works as the new public key.

35. (Previously Presented) The method of claim 33, further comprising

receiving a counter value from the mobile user device indicating the generation of private and public keys; and

generating the new public key using the previous public key and the system parameter based on the counter value.

36. (Previously Presented) A mobile user device configured for authentication in a public cryptographic system comprising:

means for creating a private key, a public key corresponding to the private key, and an associated system parameter at the mobile user device;

means for wirelessly outputting the system parameter to a verifier device concurrent with outputting the public key; and

means for using the private key for authentication of the mobile user device with the verifier device.

37. (Previously Presented) The device of claim 36, further comprising:

means for creating a new private key using a previous private key and the system parameter.

38. (Previously Presented) The device of claim 36, further comprising:

means for creating a counter value indicating the generation of public and private keys; and

means for outputting the counter value when outputting the public key.

39. (Previously Presented) The device of claim 38, further comprising:

means for creating a new private key using a previous private key and the system parameter based on the counter value.

40. (Previously Presented) An apparatus for verification in a public cryptographic system comprising:

means for wirelessly receiving a public key from a mobile user device;

means for wirelessly receiving a system parameter from a the mobile user device concurrent with receipt of the public key, the system parameter associated with the public key;

means for authenticating the mobile user device using the public key; and

means for generating a new public key at the verifier device and authenticating the mobile user device using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

41. (Previously Presented) The apparatus of claim 40, wherein generating the new public key comprises:

means for using a number of powers of the previous public key for authentication of the mobile user device; and

means for accepting one that works as the new public key.

42. (Previously Presented) The apparatus of claim 40, further comprising

means for receiving a counter value from the mobile user device, the counter value indicating the generation of private and public keys; and

means for generating the new public key using the previous public key and the system parameter based on the counter value.

43. (Previously Presented) A machine-readable medium comprising instructions operational in a mobile user device for performing a public cryptography, which when executed by a processor causes the processor to:

create a private key and corresponding public key with an associated system parameter on the mobile user device;

wirelessly output the system parameter to a verifier device concurrent with wirelessly outputting the public key to the verifier device; and

use the private key for authentication of the mobile user device.

44. (Previously Presented) The machine-readable medium of claim 43 further comprising instructions to:

create a new private key at the mobile user device using a previous private key and the system parameter.

45. (Previously Presented) The machine-readable medium of claim 43 further comprising instructions to:

create a counter value indicating the generation of public and private keys; and

output the counter value when outputting the public key.

46. (Previously Presented) The machine-readable medium of claim 45 further comprising instructions to:

create a new private key using a previous private key and the system parameter based on the counter value, if the previous private key is not active.

47. (Previously Presented) A machine-readable medium comprising instructions for performing a public cryptography at a verifier device, which when executed by a processor causes the processor to:

wirelessly receive a public key from a mobile user device;

wirelessly receive a system parameter from the mobile user device concurrent with receipt of the public key, the system parameter associated with the public key;

authenticate the mobile user device using the public key;

generate a new public key at the verifier device and authenticate the mobile user device using the new public key, if a previous public key fails, the new public key being derived from the previous public key and the system parameter.

48. (Previously Presented) The machine-readable medium of claim 47 further comprising instructions to:

use a number of powers of the previous public key for authentication of the mobile user device; and

accept one that works as the new public key for the mobile user device.

49. (Previously Presented) The machine-readable medium of claim 47 further comprising instructions to:

receive a counter value indicating the generation of private and public keys from a mobile user device; and

generate the new public key using the previous public key and the system parameter based on the counter value.

50. (Currently Amended) A mobile user device used for authentication comprising:

a processor configured to generate a first private key and corresponding first public key, the processor configured to generate a second private key associated with the first private key and to create a second public key corresponding to the second private key;

a storage medium coupled to the processor, configured to store the first private key; and

a wireless transmitter coupled to the processor to output a plurality of shares of the second private key to a plurality of different entities once such that ~~it~~ the second private key can be re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created and output the second public key to the verifier device concurrent with wirelessly outputting the first public key;

wherein the processor uses the first private key for authentication of the mobile user device.

51. (Currently Amended) Apparatus used for verification comprising:

a receiver configured to

wirelessly receive a first public key from a mobile user device and to receive a second public key from the mobile user device concurrent with receipt of the first public key, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities, where each share is sent only once and to a different entity, such that the second private key can be re-created by the mobile user device to

replace use of a first private key corresponding to the first public key and disable the first private key when the second private key is re-created;

a storage medium coupled to the receiver, configured to store the first and second public keys; and

a processor coupled to the receiver, the processor configured to use the first public key for authentication of the mobile user device, the processor configured to use the second public key for authentication of the mobile user device if the first public key fails.